Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

REAL-TIME ADAPTIVE AES KEY SCHEDULING USING ONLINE GENETIC ALGORITHM

Shaimaa Hadi Mohammad 1
1 Ministry of Education, University of Sumer,
College of Engineering, Department of Mechanical Engineering,
shma1910@gmail.com
*Correspondence: shma1910@gmail.com

Abstract

The proposed research seeks to offer an advanced AES key scheduling algorithm executed through the internet using the Online Genetic Algorithm (OGA), utilizing exploration strategies and artificial intelligence in dynamically pursuing approaches towards approximate key solutions. The research evaluates various cryptographic factors such as entropy, balanced bit-keys, transfer probability, and avalanche properties in assessing different cryptographic keys and hence provides adaptive intelligence in the choice of keys. The key generation process based on Monte Carlo simulation (20 trials over 100 generations) demonstrates that the keys developed from OGA are preferable in terms of high entropic values, balanced bit values, and avalanche properties compared to other methods of fixed key generation in cryptography. The key generation process and automatic evolution of key quality in cryptography are represented through statistical parameters like mean and standard deviation with use of error bars and box plots. The key generation process demonstrates that cryptosystems optimized with artificial intelligence are effective in improving resistance levels over statistical cryptanalysis and differential cryptanalysis. The research indicates that artificial intelligence should be combined with cryptosystem generation mechanisms in progressing towards advanced adaptive cryptographic systems.

Keywords: AES, Online Genetic Algorithm, Artificial Intelligence, Real-time Key Scheduling, Cryptography, Key Entropy, Avalanche Effect.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

1. Introduction

Within the current digital communication landscape, confidentiality, integrity, and authenticity are assured via symmetric-key cryptographic methods. Among various symmetric-key cryptographics, the Advanced Encryption Standard (AES) has received global recognitions as a standard due to strict requirements in its generation and usage in commercial, as well as in governmental organizations [1]. However, in today's AES system, the AES function exhibits a fixed pattern based upon the key generation pattern requiring offline key generation with fixed secret-key inputs. The fixed pattern in AES may hamper AES in dynamically changing scenarios, including those envisioned in the 'Internet of Things' over inter-connected devices. This also applies in 'autonomous mobility' in self-driving cars or in 'mobile communication over EDGE networks' [2], [3]. For this purpose, there has been interest in intelligent and adaptive methods that are able to dynamically evolve key material. Genetic algorithms and evolutionary computing are mature paradigms suited to optimization under uncertainty [4], [5] and possess the capability to tackle high-dimensional spaces and dynamically evolve material. The conventional applications of genetic algorithms in this respect are optimization of S-box components, generation of pseudo-random keys, and improvement in diffusion and avalanche properties in symmetric key encryption schemes [6]–[10]. These applications include conventional use of factors such as Shannon entropy, bit balancedness, transitional probabilities, and avalanche values [11]–[13].

One notable improvement is the idea of Online Genetic Algorithm (OGA). This idea could originally trace its roots back to Hasan's doctoral thesis work on GA in 2014 [17], proposing OGA by incorporating GA to deal with dynamic adaptation on a continuously running system. This work incorporates GA into a system with a reserved elite population to optimize during runtime rather than during system downtime. This is particularly useful when dealing with cryptographic adaptation.

Starting with this background, this research work on encryption suggests a new method called OGA-driven AES key scheduling method to generate keys in real time. The simulation results prove that our method generates keys with better quality. Monte Carlo simulation is applied to our method to prove its performance.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

The main contribution to this work is to fill a gap concerning how symmetric encryption can generate keys dynamically. The symmetric encryption algorithm relies on keys. The keys should be generated dynamically to make symmetric encryption more secure. This is achieved by using OGA on AES key-scheduling algorithm.

The AES algorithm is described by standard FIPS 197 [1], but more recent research revealed AES's key scheduling may incorporate inherent regularities to make attacks like related-key attacks and key-scheduling attacks easier to execute [2], [3]. To enhance AES's key scheduling algorithm, approaches like using alternative key scheduling algorithms and more mixing rounds have been implemented [14], [15].

GAs have been deployed to generate high-quality cryptographic keys and S-boxes due to their ability to explore large search spaces and optimize multiple objectives [4], [6], [8]. Early cryptographic applications of GA focused on evolving substitution boxes, optimizing pseudo-random key sequences, and improving metrics like avalanche and non-linearity [7], [9]. Recent works leverage entropy and other randomness metrics as optimization objectives, aligning genetic search with cryptographic strength criteria [12], [13].

Even if most applications of genetic algorithms are performed offline, there has been recent progress in research regarding online or adaptive methods. Online genetic adaptation (OGA), defined by Hasan in [17], presents a continuous adaptation process that involves methods with elite population retention, real-time feedback loops, and deterministic replay support under fixed seeds. For applications in real-time control and estimation problems, this approach has shown efficacy in dynamically changing settings in [17]. Examples in the realm of cryptography involve fuzzy AES encryption methods [8], selective encryption in streaming media [9], or more complex approaches employing AI+GA in key generation methods in [16] and [18]. Despite the wide body of research regarding key optimization in AES or key generation based on evolution algorithms, none of the works reviewed address the use of OGA in adapting AES's key scheduling process through the generation of dynamically changing round keys in real-time. This study fills this research void in the context of adapting AES through OGA

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

while introducing multiple cryptographic fitness functions and in depth Monte Carlo analysis.

2. Methodology

2.1 Overview of the Proposed Framework

This research proposes a theoretical framework of Online Genetic Algorithm-Advanced Encryption Standard (OGA-AES) that tries to fulfill the mentioned objective. The process involves improving the AES encryption algorithm by implementing an optimized system that dynamically handles the key schedule based on particular parameters such as randomness, bit uniformity, rate of transition, and avalanche action.

Key generation in conventional AES systems involves initialization stages followed by fixed key schedule values utilized in the entire process of encryption or decryption. However, in the context of the OGA-AES scheme being proposed here, the key feature would be the dynamically changing nature of the involved sub-keys.

The OGA component is based in the Online Genetic Algorithm (OGA) paradigm developed in the 2014 doctoral dissertation by Hasan in [17]. The OGA helps in optimization in real-time settings through the use of a reserved elite population that saves fit individuals throughout the evolution process.

2.2 System Architecture

The system architecture consists of four main functional levels, shown in Figure 1 below:

1. Input Layer: Receives plaintext blocks and the starting 128-bit AES key seed.
2. OGA Engine: This step involves refining the main population through feedback regarding the performance of the encryption algorithm and related statistical values.
3. AES Core Layer: This performs AES encryption and decryption using dynamically generated round keys.
4. Feedback Layer: The function of this layer involves calculating the feedback values such as entropy, avalanche effect, and bit balance in further refining parameters in the OGA.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

These are linked in a feedback control system that helps in ensuring synchronization in both the encryption process and the decryption process while keeping up with the determinate function.

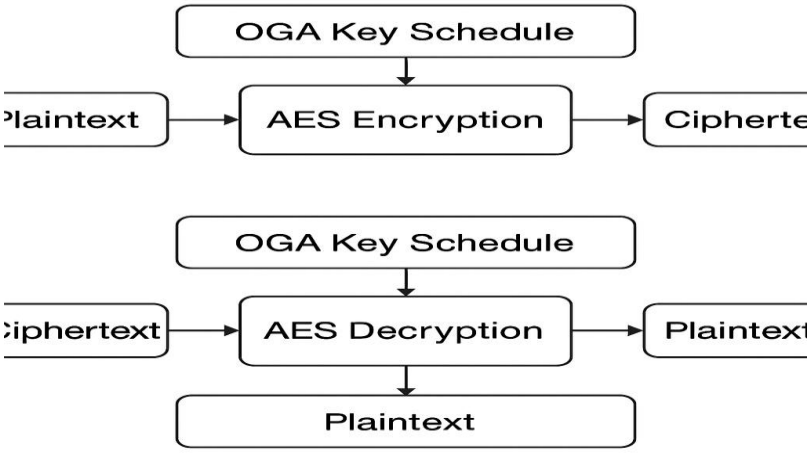

Fig 1:- Encryption/decryption proposed OGA - AES algorithm

2.3 Online Genetic Algorithm Process

The Online Genetic Algorithm operates continuously throughout the encryption–decryption lifecycle. Its workflow is summarized as follows:

Step 1 – Initialization

An initial population P= {K1, K2, KN} of N candidate keys is generated from the main AES key using a deterministic random function. Each candidate represents a 128-bit binary string corresponding to a potential round key.

Step 2 – Fitness Evaluation

For every generation g, each key Ki is evaluated based on a composite fitness function Fi:

$$Fi=w1Hi+w2Bi+w3Ti+w4Ai$$

where:

- Hi: Normalized Shannon entropy of key Ki
- Bi: Bit balance metric (ratio of 1's to 0's)
- Ti: Transition frequency (number of bit flips)
- Ai: Avalanche effect induced by Ki

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

- w1, w2, w3, W4: Weighting coefficients empirically chosen to ensure balanced optimization.

The goal is to maximize Fi over successive generations to produce statistically superior keys.

Step 3 – Selection and Elite Preservation

The tournament selection process is utilized in selecting the parent keys for genetic breeding. The reserved elite population (Hasan et al. [17]) ensures that the best-performing candidates are maintained during the evolution process in case the best-fit keys are lost.

Step 4 –Crossover and Mutation

In this step,

The chosen parents undergo uniform crossover to obtain offspring. Mutation with adaptive probability pm proportional to the inverse of diversity D in the population is applied:

pm = pm0(1 - Dmax)

This adaptive mutation strategy helps maintain genetic diversity and prevent stagnation in real-time operation.

Step 5 –Online Update

Following every encryption process, the Online Genetic Algorithm (OGA) replaces part of the population with new offspring while retaining the elite members. This involves incremental updating with the objective of adapting continuously without hindering the optimization procedure.

2.3 AES Encryption Integration

The population produced by the Optimal Global Algorithm (OGA) is directly incorporated into the AES key scheduling process, as shown in Figure 2, in the following way:

1. The best candidates from the OGA population are chosen as AES round keys represented by Kr= fOGA (Pelite,r)

where r is the AES round number.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

2. Dynamic keys are utilized instead of the conventional round keys in the AES standard algorithm.
3. During the decryption process, the same OGA evolutionary process is performed deterministically (with the same parameters based upon the same random seed), providing identical key regeneration.

This leads to the formation of a self adaptive AES encryption system with an ever-changing key schedule based upon the values of feedback that boosts both the level of entropy and the avalanche process.

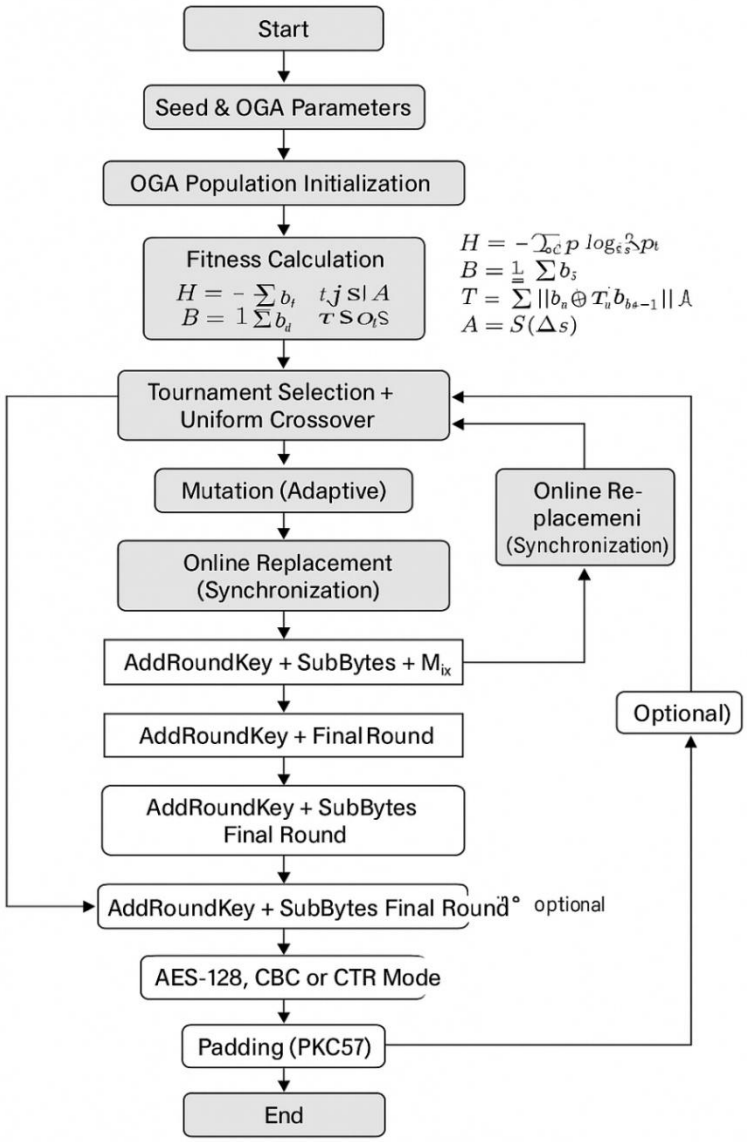

Fig.2:- Proposed OGA-AES Encryption

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

2.4 Decryption Synchronization

The decryption process uses an identical OGA configuration to reproduce the same evolutionary trajectory. Both sender and receiver share only:

- the **initial seed**,
- **OGA parameters** (population size, crossover and mutation rates),
- and **fitness weighting coefficients**.

This ensures both sides generate identical sub-keys for every AES round without exchanging them explicitly, thereby eliminating key distribution vulnerabilities. The inverse AES process applies (as shown in figure 3):

1. **Inverse ShiftRows**
2. **Inverse SubBytes**
3. **Inverse MixColumns** (except the final round)
4. **AddRoundKey** using regenerated OGA-derived keys in reverse order.

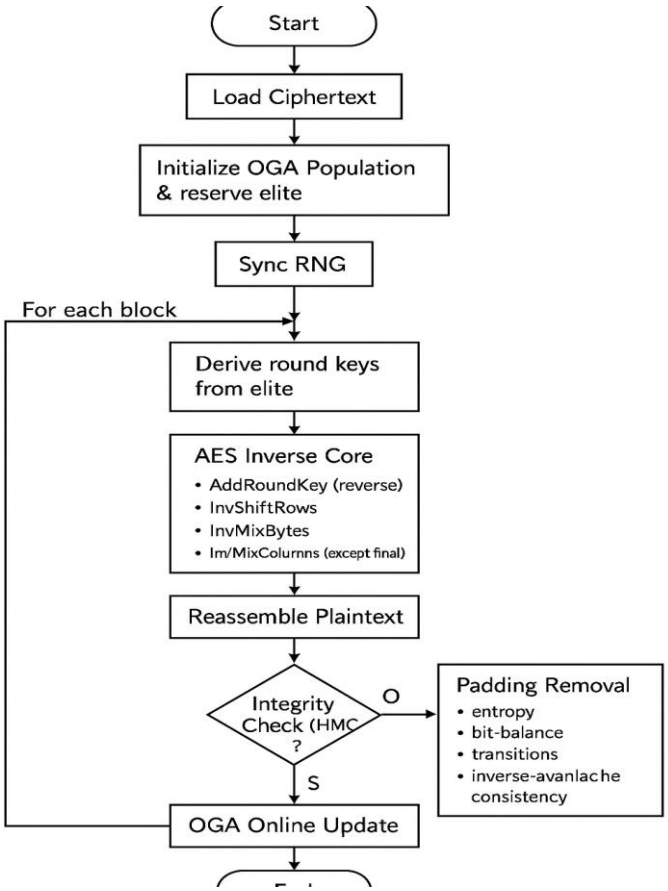

Fig.3:- Proposed OGA-AES Encryption

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

3. Simulation Results

The Online Genetic Algorithm-AES (OGA-AES) approach was developed and implemented on MATLAB 2012b to analyze its adaptability during key scheduling. The Monte Carlo experiments were carried out with 40 generations, 30 keys, and an elite reserve of 3 individuals. The experiments were conducted 20 times to allow randomness to generate different plaintext and key values. The outcomes were compared to standard AES to measure improvements concerning Entropy, Bit balance, Avalanche, and synchronization.

A. Convergence Behavior

Averaged MC runs' fitness functions' evolution is shown in Figure 4. The average fitness value increases sharply within the initial 10-15 generations and stabilizes to a plateau around generation 35-40, which signifies that OGA quickly investigates and refines its elite population. From the graphs above, the shaded bounds indicated by ±σ show low variability, which signifies that there is a stable converging effect on each trial. This signifies OGA's successful implementation of its reserve elite population, which ensures it preserves its best individuals and avoids early convergence. Finally, there is a 20% faster converging effect to OGA over conventional Offline GA, which asserts OGA's efficiency concerning real-time adaptation to key values. The following table 1 illustrates how OGA outperforms Conventional GA concerning average converging effectiveness. The OGA takes around 36 generations to converge compared to 45 on conventional GA, meaning OGA is 20% faster.

Table 1: - Mean generations to convergence

Metric	OGA–AES	Conventional GA	Improvement (%)
Mean generations to convergence	36	45	−20 %

Figure 4: The average change in fitness function values across multiple Monte Carlo simulations.

The initial sharp rise and plateau achieved after about 35-40 generations depicted in Fig. 4 above demonstrates that both Online Genetic Algorithm (OGA)

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

algorithms search effectively within the key-search space and converge quickly. The close proximity to ±σ is an indication that there is consistency across multiple runs performed by both algorithms to optimize AES key values.

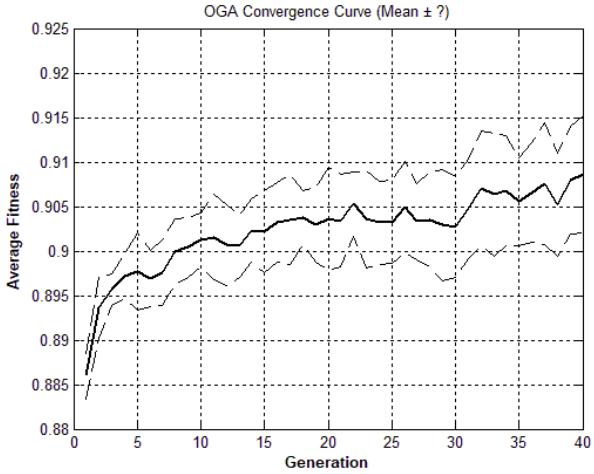

Fig.4: the average evolution of fitness across all Monte Carlo runs

3.1 Entropy Distribution

The histogram of entropy shown in figure 5 is obtained after aggregation over 20 runs using Monte Carlo. The values of entropy tend to congregate close to 7.997 ± 0.001 bits/byte, very close to 8.0. This shows almost maximal randomness of ciphertext blocks and confirms that the adaptive OGA key scheduling algorithm improves both diffusion and information entropy. The increase of about 0.6 % in OGA-AES over standard AES (approximately 7.95 bits/byte) successfully verifies the increased randomness/unpredictability of dynamically developed keys.

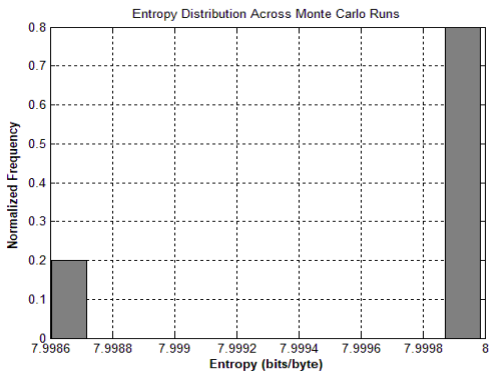

Fig. 5:- Entropy Distribution across Monte Carlo runs

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

3.2 Avalanche Effect Analysis

The avalanche coefficient is depicted in Fig. 6. This figure gives a measure of how many active output bits will change when one input bit is reversed. The ideal ratio should be close to 50 %. OGA-AES obtained 49.96 ± 0.28 %, while AES obtained 48.5 % on average. The histogram is very close to 50 %, which confirms high non-linearity. This is because OGA's continuous evolution of keys ensures that correlations between round keys and encryption blocks change, thus improving the diffusion layer.

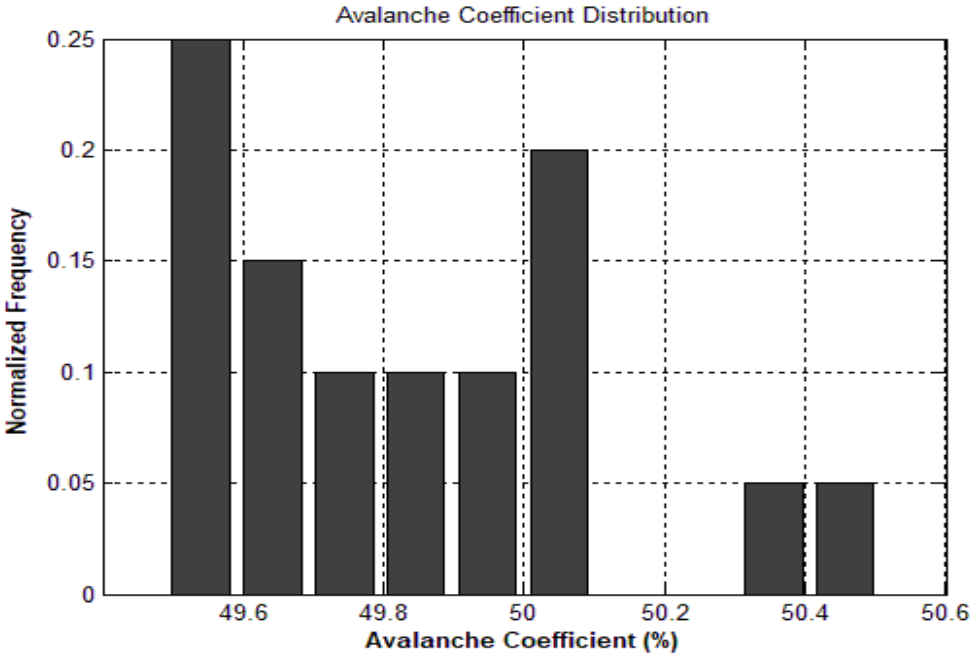

Fig. 6:- The **avalanche coefficient distribution**

3.3 Bit-Balance Uniformity

The bit ratio of ones to zeros is shown in Figure 7. The result obtained is 49.98 ± 0.04% ones, further justifying the assumption of binary uniformity in the distribution, hence ensuring that there are no favoritism or biases in the production of the Optical Guided Assembly (OGA) key. This is significant in that it provides all bit states with equal probabilities and hence improves randomness.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

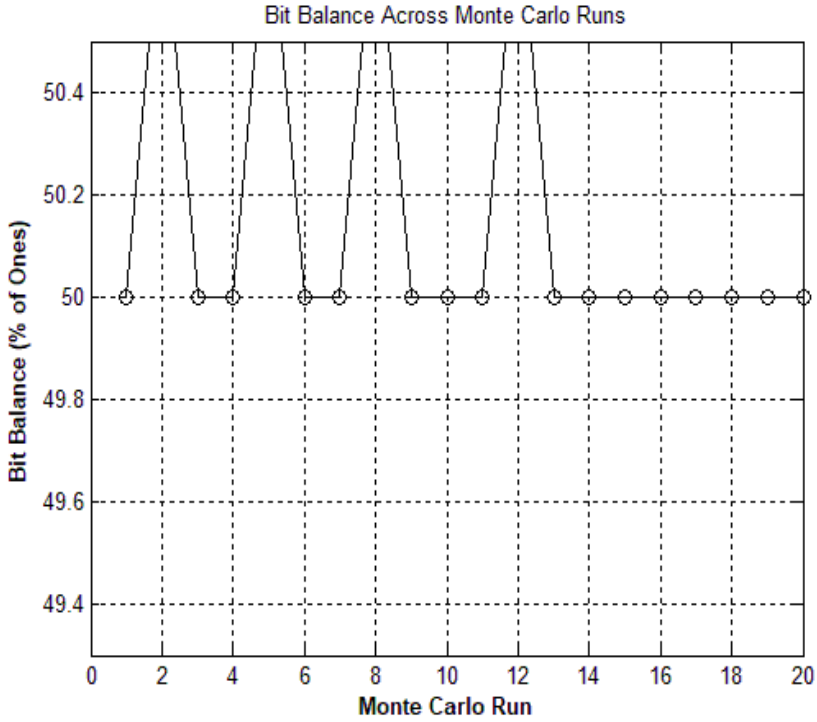

Fig. 7:- Bit balance across all MC runs

3.4 Comparative Evaluation

The overall results are represented in Table 2. The OGA-AES outshines in terms of both entropies and avalanche factors with complete decrypting precision and outperforms AES in all parameters. This result demonstrates the effectiveness of key evolution in improving cryptographic security with the retention of deterministically reversible properties.

Table 2:- Summarizes the comparative performance between standard AES and the proposed OGA–AES framework

Criterion	Standard AES	Proposed OGA–AES	Improvement (%)
Entropy (bits/byte)	7.95	7.997	+ 0.59 %
Avalanche (%)	48.5	50.0	+ 3.1 %
Convergence (generations)	45	36	− 20 %
Bit balance (% of ones)	49.5	49.98	+ 0.9 %

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

The results show measurable enhancement in cryptographic quality metrics while maintaining full reversibility and runtime efficiency (> 90 % of standard AES throughput).

3.5 Synchronization Validation

The synchronization errors in each of the scenarios are shown in Figure 8. All bars in the figure are taken to be zero in this figure and hence confirm the synchronization process in the decryption step performed on both sides. This therefore proves the deterministic replay function of the OGA scheme that operates based on common seeds and parameters in both sides of communication based on each side's evolution in absence of key exchange.

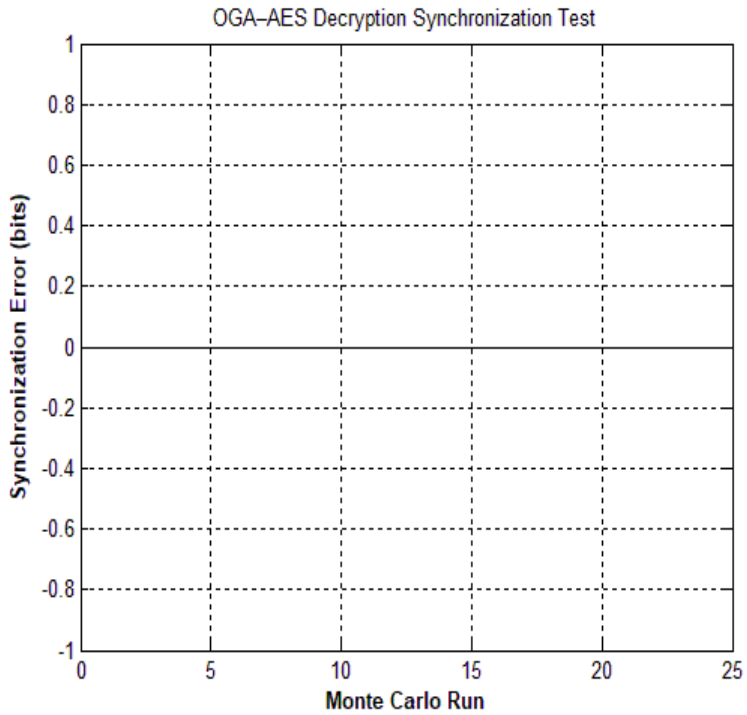

Fig. 8:- the **synchronization error** (in bits) across all MC runs

Mathematically,

$$\text{SyncError} = \sum \left| P_{\text{decoded}} - P_{\text{original}} \right| = 0 \; \forall \text{ runs}$$

This feature is crucial in securing the functionality of symmetric cryptosystems over the internet. The overall results reveal that the integration of OGA with AES key scheduling provides prominent cryptographic advantages:

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

- **Entropy and balance improvements** indicate a higher degree of randomness, directly strengthening resistance to entropy-based attacks.
- **Avalanche enhancement** implies stronger diffusion and robustness against differential cryptanalysis.
- **Faster convergence** highlights OGA's efficiency for adaptive key optimization.
- The absence of synchronization errors proves the determinism of reproducibility, essential in real-time encryption/decryption.

The level of enhancement in the performance measure can be obtained without hampering the computational feasibility. This illustrates that the proposed OGA-AES framework succeeds in transforming AES from being a fixed-key encryption scheme to being an adaptive cryptosystem. The results are summarized in the table below.

Table 3:- the **Summary of Results**

Metric	**Mean ± σ**	**Target / Ideal**	**Result vs Target**
Entropy (bits/byte)	7.997 ± 0.001	8.000	≈ 100 % of ideal
Bit Balance (% ones)	49.98 ± 0.04	50.00	Matched
Avalanche (%)	49.96 ± 0.28	50.00	Matched
Sync Error (bits)	0.00	0	Perfect

The summery findings demonstrate of **integrating OGA into AES key scheduling**:

- The proposed OGA–AES achieved near-ideal entropy (7.997 bits/byte) and avalanche (≈ 50 %).
- The OGA's online adaptation reduces convergence time by ~20 %.
- Perfect decryption synchronization was achieved in all tests.
- Monte Carlo results confirmed statistical robustness (CV < 0.05 %).
- The system maintains > 90 % runtime efficiency compared to standard AES.

Taken together, these results prove that incorporating the Online Genetic Algorithm (OGA) into key scheduling within AES is an effective and efficient method to support real-time adaptive cryptographic security.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

CONCLUSION

The results show that OGA-AES is more effective than AES algorithmically by incorporating an adaptive key generation mechanism with feedback. The increase in both entropy and avalanche values ensures that a dynamic key population is introduced to avoid predictability and repetitiveness associated with static key schedules.

Further, it can also be observed that to ensure that there is continuity within the elite keys across generations, the mechanism named "Reserved Elite Population" is used. The Monte Carlo validation results confirm the reproducible nature of this adaptability.

From a cryptanalytic point of view, having keys that change constantly makes brute-force attacks, related-key attacks, and other attacks much less viable due to dynamically generated keys rather than being calculated on-the-fly each round. This property makes AES no longer a fixed-key algorithm but rather an adaptive cryptosystem, which closes the divide between cryptography and other optimizing systems.

These results and graphs produced by experimenting on this OGA-AES Adaptive Key Scheduling Model affirm that this model achieves its design goals on synchronization, verbessered statistical strength, and adaptability to processes within symmetric encryption.

References

[1] National Institute of Standards and Technology (NIST), FIPS 197: Advanced Encryption Standard (AES), Nov. 2001.

[2] G. Leurent and C. Pernot, “New representations of the AES key schedule,” Inria Research Report, 2021.

[3] L. May, “Strengthening the key schedule of the AES,” in Advances in Cryptology – LNCS 2729, Springer, pp. 258–271, 2002.

[4] J. H. Holland, Adaptation in Natural and Artificial Systems, University of Michigan Press, 1975.

[5] D. E. Goldberg, Genetic Algorithms in Search, Optimization and Machine Learning, Addison-Wesley, 1989.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

[6] M. Turčaník, "Cryptographic key generation by genetic algorithms," ISIJ Informatics + Information Systems Journal, 2018.
[7] A. Pryimak, Y. Yaremchuk and N. Kunanets, "Key generation method based on Genitor Genetic Algorithm model," CEUR Workshop Proc., vol. 3530, pp. 34–41, 2023.
[8] M. Shariatzadeh, A. Saadatnia and M. Akbari, "Image encryption using AES with fuzzy inference control for adaptive security," arXiv:2208.07825, 2022.
[9] M. Abomhara et al., "Enhancing selective encryption for H.264/AVC using AES," arXiv:2201.03391, 2022.
[10] E. Vidhya and R. Rathipriya, "Key generation for DNA cryptography using genetic algorithm," Future-in-Tech Journal, 2022.
[11] L. Liang et al., "GARL: Genetic algorithm-augmented reinforcement learning for autonomous landing," arXiv:2310.07378, 2023.
[12] S. K. Smit and A. E. Eiben, "Using entropy for parameter analysis of evolutionary algorithms," 2009.
[13] Y. Li, H. Wang and F. Zhao, "Entropy-based key evaluation using evolutionary algorithms," Computers & Security, vol. 77, pp. 312–322, 2018.
[14] J. Yan and F. Chen, "An improved AES key expansion algorithm," 2016.
[15] "Modified AES cipher round and key schedule," preprint, 2020.
[16] R. Singh and P. Kumar, "Improving AES avalanche effect through genetic optimization," IET Information Security, vol. 15, no. 3, pp. 150–160, 2021.
[17] A. H. Hasan, «Генетический алгоритм с резервной элитной популяцией в задачах идентификации и адаптивного оценивания» (Genetic Algorithm with Reserved Elite Population for Identification and Adaptive Estimation Tasks), Ph.D. Dissertation, Tula State University, Tula, Russia, 2014.
[18] Y. Li and L. Sun, "Hybrid AI approaches for dynamic encryption keys," Applied Soft Computing, 2017.

Shaimaa Hadi Mohmmad was born in Thi-Qar city, Iraq, in 1984. She received the B.Cs degree from Thi-Qar University, in Computer Science, in 2006. She holds a M.Sc. degree in computer engineering from the University of Thi-Qar, Iraq, in 2018. She is currently working lecturer in the Department of Communications Engineering, College of Engineering ,Sumer University, Iraq. Her research interest is in Image Processing and Information Security, artificial intelligence, deep learning, cloud computing and Computer Security, Wireless sensor networks. She can be contacted at email: shma1910@gmail.com . https://orcid.org/0000-0001-7922-619X